changes may take place when the submitter requests in writing that the information no longer be protected under the CII Act of 2002 or when the Protected CII Program Manager or the Protected CII Program Manager's designee determines that the information was customarily in the public domain, is publicly available through legal means, or is required to be submitted to DHS by Federal law or regulation. The Protected CII Program Manager or the Protected CII Program Manager's designees shall inform the submitter when a change in status is made. Notice of the change in status of Protected CII shall be provided to all recipients of that Protected CII under § 29.8.

§ 29.7 Safeguarding of Protected Critical Infrastructure Information.

(a) *Safeguarding.* All persons granted access to Protected CII are responsible for safeguarding all such information in their possession or control. Protected CII shall be protected at all times by appropriate storage and handling. Each person who works with Protected CII is personally responsible for taking proper precautions to ensure that unauthorized persons do not gain access to it.

(b) *Use and storage.* When Protected CII is in the physical possession of a person, reasonable steps shall be taken to minimize the risk of access to Protected CII by unauthorized persons. When Protected CII is not in the physical possession of a person, it shall be stored in a secure environment that affords it the necessary level of protection commensurate with its vulnerability and sensitivity.

(c) *Reproduction.* Pursuant to procedures prescribed by the Protected CII Program Manager, a document or other material containing PCII may be reproduced to the extent necessary consistent with the need to carry out official duties, provided that the reproduced documents or material are marked and protected in the same manner as the original documents or material.

(d) *Disposal of information.* Documents and material containing Protected CII may be disposed of by any method that prevents unauthorized retrieval.

(e) *Transmission of information.* Protected CII shall be transmitted only by secure means of delivery as determined by the Protected CII Program Manager or the Protected CII Program Manager's designees.

(f) *Automated Information Systems.* The Protected CII Program Manager or the Protected CII Program Manager's designees shall establish security requirements for Automated Information Systems that contain Protected CII.

§ 29.8 Disclosure of Protected Critical Infrastructure Information.

(a) *Authorization of access.* The Under Secretary for IAIP, or the Under Secretary's designee, may choose to provide or authorize access to Protected CII when it is determined that this access supports a lawful and authorized Government purpose as enumerated in the CII Act of 2002, other law, regulation, or legal authority. Any disclosure or use of Protected CII within the Federal government is limited by the terms of the CII Act of 2002. Accordingly, any advisories, alerts, or warnings issued to the public pursuant to paragraph (e) of this section shall protect from disclosure:

(1) The source of any voluntarily submitted CII that forms the basis for the warning, and

(2) Any information that is proprietary, business sensitive, relates specifically to the submitting person or entity, and is not customarily in the public domain.

(b) *Federal, State, and local government sharing.* The Protected CII Program Manager or the Protected CII Program Manager's designees may provide Protected CII to an employee of the Federal government, or of a State or local government, provided that such information is shared for purposes of securing the critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or for another informational purpose including, without limitation, the identification, analysis, prevention, preemption, and/or disruption of terrorist threats to our homeland. Protected CII may be provided to a State or local government entity only pursuant to its express written

agreement with the Protected CII Program Manager to comply with the requirements of paragraph (d) of this section and that acknowledges the understanding and responsibilities of the recipient.

(c) *Disclosure of information to Federal contractors.* Disclosure of Protected CII to Federal contractors may be made only after the Protected CII Program Manager or a Protected CII Officer certifies that the contractor is performing services in support of the purposes of DHS, the contractor has signed corporate or individual confidentiality agreements as appropriate, covering an identified category of contractor employees where appropriate, and has agreed by contract to comply with all the requirements of the Protected CII Program. The contractor shall safeguard Protected CII in accordance with these procedures and shall not remove any "Protected CII" markings. Contractors shall not further disclose Protected CII to any of their components, additional employees, or other contractors (including subcontractors) without the prior written approval of the Protected CII Program Manager or the Protected CII Program Manager's designees, unless such disclosure is expressly authorized in writing by the submitter and is the subject of timely notification to the Protected CII Program Manager.

(d) *Further use or disclosure of information by State and local governments.* (1) State and local governments receiving information marked "Protected Critical Infrastructure Information" shall not share that information with any other party, or remove any Protected CII markings, without first obtaining authorization from the Protected CII Program Manager or the Protected CII Program Manager's designees who shall be responsible for requesting and obtaining written consent for any such State or local government disclosure from the person or entity that submitted the information or on whose behalf the information was submitted.

(2) The Protected CII Program Manager or a Protected CII Program Manager's designee may not authorize State and local governments to further disclose the information to another party unless the Protected CII Program Manager or a Protected CII Program Manager's designee first obtains the written consent of the person or entity submitting the information.

(3) State and local governments may use Protected CII only for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act.

(e) *Disclosure of information to appropriate entities or to the general public.* The IAIP Directorate may provide advisories, alerts, and warnings to relevant companies, targeted sectors, other governmental entities, ISAOs or the general public regarding potential threats and vulnerabilities to critical infrastructure as appropriate. In issuing a warning, the IAIP Directorate shall protect from disclosure the source of any Protected CII that forms the basis for the warning as well as any information that is proprietary, business sensitive, relates specifically to the submitting person or entity, and is not customarily in the public domain.

(f) *Access by Congress and whistleblower protection.* (1) Exceptions for disclosure.

(i) Pursuant to section 214(a)(1)(D) of the CII Act of 2002, Protected CII shall not, without the written consent of the person or entity submitting such information, be used or disclosed by any officer or employee of the United States for purposes other than the purposes of the CII Act of 2002, except—

(A) In furtherance of an investigation or the prosecution of a criminal act; or

(B) When disclosure of the information is made—

(*1*) To either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee thereof or subcommittee of any such joint committee; or

(*2*) To the Comptroller General, or any authorized representative of the Comptroller General, in the course of the performance of the duties of the General Accounting Office.

(ii) If any officer or employee of the United States makes any disclosure pursuant to these exceptions, contemporaneous written notification must be provided to the Department through the Protected CII Program Manager.

(2) Consistent with the authority to disclose information for any purpose described in §29.2, disclosure of Protected CII may be made, without the written consent of the person or entity submitting such information, to the DHS Inspector General, or to any other employee designated by the Secretary of Homeland Security.

(3) Subject to the limitations of title 5 U.S.C., section 1213 (the "Whistleblower Protection Act"), disclosure of Protected CII may be made by any officer or employee of the United States who reasonably believes that such information:

(i) Evidences an employee's or agency's conduct in violation of criminal law, or any other law, rule, or regulation, affecting or relating to the protection of the critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, or reconstitution or

(ii) Evidences mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety affecting or relating to the protection of the critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, or reconstitution.

(4) Disclosures of all of the information cited in paragraphs (f)(1) through (3) of this section, including under paragraph (f)(1)(i)(A), are authorized by law and therefore are not subject to penalty under section 214(f) of the Homeland Security Act of 2002.

(g) *Responding to requests made under the Freedom of Information Act or State/local information access laws.* (1) Protected CII shall be treated as exempt from disclosure under the Freedom of Information Act and, if provided by the Protected CII Program Manager or the Protected CII Program Manager's designees to a State or local government agency, entity, or authority, or an employee or contractor thereof, shall not be made available pursuant to any State or local law requiring disclosure of records or information. Any Federal, State, or local government agency with questions regarding the protection of Protected CII from public disclosure shall contact the Protected CII Program Manager, who shall in turn consult with the DHS Office of the General Counsel.

(2) These procedures do not limit or otherwise affect the ability of a State or local government entity, agency, or authority to obtain under applicable State or local law information directly from the same person or entity voluntarily submitting information to DHS. Information independently obtained by a State or local government entity, agency, or authority is not subject to the CII Act of 2002's prohibition on making such information available pursuant to any State or local law requiring disclosure of records or information.

(h) *Ex parte communications with decisionmaking officials.* Pursuant to section 214(a)(1)(B) of the Homeland Security Act of 2002, Protected CII is not subject to any agency rules or judicial doctrine regarding ex parte communications with a decision making official.

(i) *Restriction on use of Protected CII in civil actions.* Pursuant to section 214(a)(1)(C) of the Homeland Security Act of 2002, Protected CII shall not, without the written consent of the person or entity submitting such information, be used directly by any Federal, State, or local authority, or by any third party, in any civil action arising under Federal or State law if such information is submitted in good faith under the CII Act of 2002.

(j) *Disclosure to foreign governments.* The Protected CII Program Manager or the Protected CII Program Manager's designees may provide Protected CII to a foreign Government without the written consent of the person or entity submitting such information to the same extent, and under the same conditions, it may provide advisories, alerts, and warnings to other governmental entities as described in paragraph (e) of this section, or in furtherance of an investigation or the prosecution of a criminal act. Before disclosing Protected CII to a foreign government, the Protected CII Program Manager or the Protected CII Program Manager's designees shall protect from disclosure the source of the Protected CII, any information that is proprietary or business sensitive, relates specifically to the

submitting person or entity, or is otherwise not appropriate for such disclosure.

(k) *Obtaining written consent for further disclosure from the person or entity submitting information.* (1) Authority to Seek and Obtain Submitter's Consent to Disclosure. The Protected CII Program Manager or any Protected CII Program Manager's designee may seek and obtain written consent from persons or entities submitting information when such consent is required under the CII Act of 2002 to permit disclosure. In exigent circumstances, and so long as contemporaneous notice is provided to the Protected CII Program Manager or the Protected CII Program Manager's designees, any Federal government employee may seek the consent of the submitting party to the disclosure of Protected CII where such consent is required under the CII Act of 2002.

(2) Consequence of Consent. Whether given in response to a request from the Protected CII Program Manager, the Protected CII Program Manager's designees, or another Federal government employee pursuant to paragraph (k)(1) of this section, a person's or entity's consent to additional disclosure, if conditioned on a limited release of Protected CII that is made for DHS's purposes and in a manner that offers reasonable protection against disclosure to the general public, shall not result in the information's loss of treatment as Protected CII.

§ 29.9 Investigation and reporting of violation of protected CII procedures.

(a) *Reporting of possible violations.* Persons authorized to have access to Protected CII shall report any possible violation of security procedures, the loss or misplacement of Protected CII, and any unauthorized disclosure of Protected CII immediately to the Protected CII Program Manager or the Protected CII Program Manager's designees who shall in turn report the incident to the IAIP Directorate Security Officer and to the DHS Inspector General.

(b) *Review and investigation of written report.* The Inspector General, Protected CII Program Manager, or IAIP Security Officer shall investigate the incident and, in consultation with the DHS Office of the General Counsel, determine whether a violation of procedures, loss of information, and/or unauthorized disclosure has occurred. If the investigation reveals any evidence of wrongdoing, DHS, through its Office of the General Counsel, shall immediately contact the Department of Justice's Criminal Division for consideration of prosecution under the criminal penalty provisions of section 214(f) of the CII Act of 2002.

(c) *Notification to originator of Protected CII.* If the Protected CII Program Manager or the IAIP Security Officer determines that a loss of information or an unauthorized disclosure has occurred, the Protected CII Program Manager or the Protected CII Program Manager's designees shall notify the submitter of the information in writing, unless providing such notification could reasonably be expected to harm the investigation of that loss or any other law enforcement, national security, or homeland security interest. The written notice shall contain a description of the incident and the date of disclosure, if known.

(d) *Criminal and administrative penalties.* As established in section 214(f) of the CII Act, whoever, being an officer or employee of the United States or of any department or agency thereof, knowingly publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law any information protected from disclosure by the CII Act of 2002 and coming to the officer or employee in the course of his or her employment or official duties or by reason of any examination or investigation made by, or return, report, or record made to or filed with, such department or agency or officer or employee thereof, shall be fined under title 18 of the United States Code, imprisoned not more than one year, or both, and shall be removed from office or employment.